(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－7977
（P2002－7977A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｓ	５Ｂ０３５
19/10		Ｈ０４Ｎ　1/387		５Ｂ０５８
Ｈ０４Ｌ　9/32		Ｇ０６Ｋ　19/00	Ｓ	５Ｃ０７６
Ｈ０４Ｎ　1/387		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４
			６７３Ｅ	

審査請求　未請求　請求項の数15　ＯＬ　（全　９　頁）　最終頁に続く

(21)出願番号　特願2000－184866(P2000－184866)

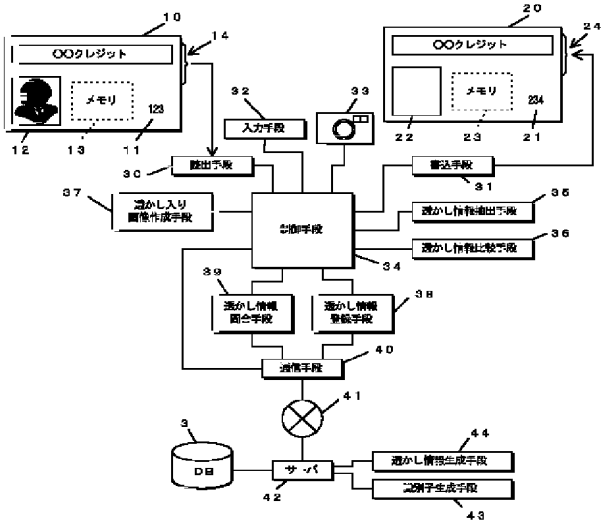
(22)出願日　平成12年６月20日(2000.6.20)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　川口　雄一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　志水　郁二
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　10009/179
弁理士　平野　一幸

最終頁に続く

(54)【発明の名称】　正当性認証システム、個人証発行システム及び個人証

(57)【要約】
【課題】　安全性が高く堅牢な正当性認証／個人証発行システムを得る。
【解決手段】　個人証の識別子と、この識別子にかかる電子透かし情報とを対応付けて記憶するデータベースと、このベースに記憶された識別子を持ち、この識別子にかかる電子透かしが埋め込まれた顔写真画像を持つ個人証を使う。個人証から顔写真画像を読み出し、データベースから個人証の識別子に対応する電子透かし情報を取り出し、読み出した顔写真画像に、取り出した電子透かし情報が埋め込まれているとき正当と判定し、そうでないとき不正と判定する。個人証と認証機器のみに依存せず、改竄に対して安全性を向上する。



【特許請求の範囲】
【請求項１】個人証の識別子と、この識別子にかかる電子透かし情報とを対応付けて記憶するデータベースと、
前記データベースに記憶された識別子を持ち、かつ、この識別子にかかる電子透かしが埋め込まれた認証画像を読み取り可能に担持する個人証と、
前記個人証から少なくとも認証画像を読み出す読出手段と、
前記データベースから前記個人証の識別子に対応する電子透かし情報を取り出す透かし情報問合手段と、
前記読出手段が読み出した認証画像に、前記透かし情報問合手段が取り出した電子透かし情報が埋め込まれているかどうか検討し、埋め込まれているとき前記個人証は正当と判定し、そうでないとき不正と判定する透かし情報比較手段とを備えたことを特徴とする正当性認証システム。
【請求項２】前記個人証には、認証画像を記憶する情報担体が設けられ、この情報担体が記憶する認証画像に、電子透かしが埋め込まれていることを特徴とする請求項１記載の正当性認証システム。
【請求項３】前記情報担体は、半導体メモリ又は磁性体の一方又は双方であることを特徴とする請求項２記載の正当性認証システム。
【請求項４】前記個人証には、認証画像を印刷した印刷物が貼り付けられ、前記読出手段は、この印刷物の画像入力を行うことを特徴とする請求項２記載の正当性認証システム。
【請求項５】前記電子透かし情報には、ランダムな値が含まれていることを特徴とする請求項１から４記載の正当性認証システム。
【請求項６】前記データベースが記憶し、かつ、前記個人証の認証画像に埋め込まれる電子透かし情報は、前記透かし情報比較手段が正当であると判定する都度、更新されることを特徴とする請求項１から５記載の正当性認証システム。
【請求項７】前記透かし情報問合手段は、通信網を介して前記データベースと通信することを特徴とする請求項１から６記載の正当性認証システム。
【請求項８】個人証に対してユニークな識別子を生成する識別子生成手段と、
前記識別子生成手段が生成した識別子に対応する電子透かし情報を生成する透かし情報生成手段と、
個人証の識別子と、この識別子にかかる電子透かし情報とを、対応付けて記憶するデータベースと、
前記識別子生成手段が生成した識別子と、前記透かし情報生成手段が生成した電子透かし情報とを、前記データベースに記憶させる透かし情報登録手段と、
生の認証画像を入力する顔画像入力手段と、
前記顔画像入力手段が入力した認証画像に、電子透かしを埋め込んだ透かし入り認証画像を作成する透かし入り画像作成手段と、
前記透かし入り画像作成手段が作成した透かし入り認証画像と、前記識別子生成手段が生成した識別子とを、読み取り可能に担持する個人証とを備えたことを特徴とする個人証発行システム。
【請求項９】前記個人証には、認証画像を記憶する情報担体が設けられ、この情報担体が記憶する認証画像に、電子透かしが埋め込まれていることを特徴とする請求項７記載の個人証発行システム。
【請求項１０】前記情報担体は、半導体メモリ又は磁性体の一方又は双方であることを特徴とする請求項９記載の個人証発行システム。
【請求項１１】前記個人証には、認証画像を印刷した印刷物が貼り付けられいることを特徴とする請求項９記載の個人証発行システム。
【請求項１２】前記電子透かし情報には、ランダムな値が含まれていることを特徴とする請求項８から１１記載の個人証発行システム。
【請求項１３】前記データベースが記憶し、かつ、前記個人証の認証画像に埋め込まれる電子透かし情報は、所定時に更新されることを特徴とする請求項１５記載の個人証発行システム。
【請求項１４】前記透かし情報登録手段は、通信網を介して前記データベースと通信することを特徴とする請求項８から１３記載の個人証発行システム。
【請求項１５】固有の識別子を持ち、かつ持ち主の認証画像が目視可能に表示される個人証であって、前記認証画像には、前記識別子に対応する電子透かし情報が埋め込まれ、しかも、この識別子と、この電子透かし情報とは、この個人証から離れたデータベースに対応付けて記憶されていることを特徴とする個人証。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、正当性認証システム、個人証発行システム及びこれらのシステムで用いられる用いられる個人証に関するものである。
【０００２】
【従来の技術】一般に、クレジットカード、キャッシュカード、会員証、学生証、社員証、パスポート、保険証、免許証などのように、認証画像を含む個人証（形態は、カード型またはブック型などがある）が、広く用いられている。ここで、本明細書において、「認証画像」とは、例えば、顔写真画像、指紋又は瞳の画像など、個人を特定できる画像をいう。
【０００３】ところが、これらの個人証の持ち主でないものが、認証画像を持ち主の認証画像から違う認証画像にすり替えて、あたかも持ち主であるかのように、なりすます事件が多発しており、社会的な問題になっている。
【０００４】これについての対策として、顔写真に電子

透かしを埋め込む技術が提案されている（特開平１０－２７５２０３号公報）。電子透かしを用いると、デジタルデータである認証画像に、所望のデータを、目では見えないように、透かし情報を埋め込むことができる。

【０００５】そして、このものでは、個人証に電子透かしを埋め込み、認証機器（カードリーダなど）側で正しく電子透かしを取り出せるかどうかにより、個人証の正当性を判断している。

【０００６】また、一般に、個人証作成時に、持ち主の識別子が「ＢＢＢ」であり、追加する情報が「ＡＡＡ」であるとき、「ＡＢＡＢＡＢ」という電子透かしが埋め込む場合を考える。

【０００７】この場合、認証時には、認証画像から、電子透かしを読み込む。読み込みに失敗すれば、不正と判断される。また、読み込みに成功しても、埋め込み時と逆の手順で、「ＡＢＡＢＡＢ」から識別子「ＢＢＢ」を除いた、情報「ＡＡＡ」を分離し、これが正しいかどうか検討される。検討の結果、正しいとされれば、正当と判断され、そうでなければ、不正と判断される。

【０００８】

【発明が解決しようとする課題】しかしながら、従来技術では、カード上のデータのみで、正当性を判断しており、電子透かしを埋め込むアルゴリズムが、漏れるか、又は、見破られてしまうと、簡単に改竄されてしまうという問題点があった。例えば、Ａさんのクレジットカードを盗んだ、犯人Ｂが、Ｂ自身の顔写真に、このアルゴリズムに従う、電子透かしを埋め込んだ顔写真を貼り、犯人Ｂが、このクレジットカードを利用して、買い物をしても、犯人Ｂの不正を暴くことができない。このように、従来技術では、セキュリティの上の問題が避けられなかった。

【０００９】そこで本発明は、安全性が高い正当性認証システム、個人証発行システム及びこれらのシステムで用いられる用いられる個人証を提供することを目的とする。

【課題を解決するための手段】本発明の正当性認証システムは、個人証の識別子と、この識別子にかかる電子透かし情報とを対応付けて記憶するデータベースと、データベースに記憶された識別子を持ち、かつ、この識別子にかかる電子透かしが埋め込まれた認証画像を読み取り可能に担持する個人証と、個人証から少なくとも認証画像を読み出す読出手段と、データベースから個人証の識別子に対応する電子透かし情報を取り出す透かし情報問合手段と、読出手段が読み出した認証画像に、透かし情報問合手段が取り出した電子透かし情報が埋め込まれているかどうか検討し、埋め込まれているとき個人証は正当と判定し、そうでないとき不正と判定する透かし情報比較手段とを備えている。

【００１０】この構成により、安全性が高く堅牢なシステムを構築できる。

【００１１】

【発明の実施の形態】請求項１、８、１５の構成によると、認証画像に埋め込まれる電子透かし情報は、個人証の認証画像にあるというだけでなく、データベースによっても、記憶されているため、データベースに記憶されている電子透かし情報と、個人証から取り出された電子透かし情報とを、比較対応することにより、正当な使用のみを許すことができる。

【００１２】例えば、犯人Ｂが盗んだ個人証の顔写真にうまく電子透かし情報を埋め込めても、データベース自体は改変されないから、データベースとの比較が不首尾に終わることとなり、犯人Ｂの不正を暴くことができる。即ち、個人証の認証画像のみに依存する場合に比べ、大幅に安全性を向上することができる。

【００１３】請求項２、９の構成によると、電子透かしが情報担体に記憶されており、デジタルデータのまま読み出すことができるため、正確に電子透かし情報の比較を行える。

【００１４】請求項３、１０の構成によると、情報担体が、半導体メモリ又は磁性体であるため、個人証の重量を大幅に増加せずとも、記憶ができる。

【００１５】請求項４、１１の構成によると、印刷物に認証画像が印刷されているため、個人証を、薄くかつ軽くすることができる。

【００１６】請求項５、１２の構成によると、電子透かし情報には、ランダムな値が含まれているため、偽造、変造を試みる輩にとって、予測不能とすることができ、改竄をより困難にすることができる。

【００１７】請求項６、１３の構成によると、データベースと個人証の、顔写真情報に埋め込まれる電子透かし情報が、正当であると判定される都度、更新されることにより、改竄に対してより強い体制がとれる。

【００１８】請求項７、１４の構成によると、通信網を介して、データベースは、個人証が利用される位置から離れた位置にあり、データーベースにアクセスできない限り、電子透かし情報が外部に漏れることはないため、システムの安全性を向上できる。

【００１９】次に図面を参照しながら、本発明の実施の形態を説明する。まず、各形態の説明に先立ち、図５を用いて、本発明による、識別子、電子透かし情報及びデータベースの関係を概説する。また以下、認証画像として、顔写真画像を用いる場合を、中心にして説明する。

【００２０】図５に示すように、個人証５には、識別子１、認証画像４が設けられる。識別子１と電子透かし情報２は、一対一に対応しており、データベース３に記憶されている。この例では、識別子１は「１２３」、電子透かし情報２は「ｈｏｇｅｈｏｇｅ」である。

【００２１】（実施の形態１）次に、図１を用いて、実施の形態１を説明する。図１は、本発明の実施の形態１におけるシステムのブロック図である。ここで、図１の

左上部に示す個人証１０は、発行済みのものであり、認証に用いられる。また、図１の右上部に表示される個人証２０は、発行用のものである。

【００２２】個人証１０は、顔写真などを表示する表示部１２と、情報担体としてのメモリ１３と、識別子１１（ここでは「１２３」）とを、具備している。

【００２３】また、メモリ１３にアクセスするために、入出力ポート１４が設けてある。ここで、画像を記憶する上で容量が十分であるならば、メモリ１３の代わりに、情報担体として、磁性ストラップなどの磁性体を用いてもよい。

【００２４】メモリ１３には、電子透かし情報が埋め込まれた認証画像が記憶されており、必要に応じて、表示部１２に表示できるようになっている。この表示部１２は、例えば、ＬＣＤなどからなる。

【００２５】また、発行用の個人証２０にも、同様に、識別子２１（ここでは「２３４」）、メモリ２３、入出力ポート２４が設けられている。以上が個人証の構成である。

【００２６】次に、本形態のシステムについて説明する。なおこのシステムは、説明の便宜上、正当性認証システム、個人証発行システムとを、組み合わせたものとなっているが、正当性認証システム、個人証発行システムは、別々に構成することもできる。

【００２７】さて、読出手段３０は、入出力ポート１４に接続されており、メモリ１３に記憶され、電子透かし情報が埋め込まれた、認証画像を読み出す。

【００２８】逆に、書込手段３１は、入出力ポート２４に接続されており、メモリ２３に電子透かし情報が埋め込まれた顔写真情報を書き込む。

【００２９】入力手段３２は、個人証の認証あるいは発行の際に必要な情報入力を受け付ける。デジタルカメラ３３は、持ち主の顔を撮影し、認証画像（デジタル）を出力する。制御手段３４は、他の各要素を制御するとともに、個人証の正当性を判断する。

【００３０】透かし情報抽出手段３５は、読み出し手段３０が読み出した認証画像から電子透かし情報のみを抽出し、制御手段３４に返す。

【００３１】透かし情報比較手段３６は、データベース３から得た透かし情報と、透かし情報抽出手段３５が抽出した透かし情報とを比較し、これらの透かし情報が一致するか否かを、制御手段３４に返す。

【００３２】透かし入り画像作成手段３７は、後述するように、サーバ４２側から得た、生成された透かし情報を、デジタルカメラ３３が撮影した認証画像に埋め込んで、電子透かしが埋め込まれた認証画像を作成する。

【００３３】透かし情報登録手段３８は、データベース３に、識別子と、これに対応する電子透かしを登録するよう求める。透かし情報問合手段３９は、データベース３に、識別子を渡し、これに対する透かし情報を問い合わせる。通信手段４０は、通信網４１を経由して、サーバ４２と通信を行う。

【００３４】サーバ４２には、識別子生成手段４３と、透かし情報生成手段４４とが設けられ、識別子生成手段４３は、データベース３をアクセスして、要求に応じ、未だ付与されていないユニークな識別子を生成する。透かし情報生成手段４４は、識別子に対応する透かし情報を作成する。

【００３５】なお、この透かし生成の方式は、任意に決定して差し支えないが、規則性のないランダムな値（例えば、乱数値）を透かし情報に含めることが望ましい。このようにすると、改竄を試みる者（犯罪者またはそのグループ）にとって、予測がきわめて困難になり、システムの安全性をより向上できる。また、典型的には、透かし情報は、データベース３にテキストデータとして記録され、認証画像には、電子透かしとして埋め込まれる。

【００３６】図１の例では、認証画像をデジタルカメラ３３で撮影して取得しているが、印刷物をイメージスキャナなどで読みとって認証画像を入力してもよい。勿論、認証画像として、顔写真画像ではなく、指紋又は瞳の画像を採用するときは、それにあわせた入力手段を用いる。

【００３７】また、識別子生成手段４３、透かし情報生成手段４４は、サーバ４２側でなく、制御手段３４側（サーバ４２から見るとクライアント側）に設けてもよい。

【００３８】（実施の形態２）次に、図２を参照しながら、実施の形態２におけるシステムについて説明する。このシステムは、個人証に、情報担体としてのメモリを設けない例であり、図１に示したものに対し、次の点が異なる。

【００３９】認証用の個人証５０には、識別子５１（ここでは「１２３」）が表示されているが、情報担体はなく、当然、入出力ポートもない。その代わり、印刷された顔写真５２が、貼り付けてある。そして、これをイメージスキャナ７０で入力するようになっている。

【００４０】また、発行用の個人証６０には、同様に、識別子６１（ここでは「２３４」）が表示されるが、メモリ、入出力ポートはなく、顔写真６２の貼付欄が形成されている。そして、プリンタ７１によって、電子透かし情報が埋め込まれた、顔写真６２が印刷され、これが上記貼付欄に貼り付けられる。その他の点は、図１の構成と同様である。

【００４１】（処理）次に、図３を参照しながら、個人証を発行する処理の流れを説明する。なお、実施の形態２については、処理自体において、認証画像の読み出し・書き込みの要領が違うだけであり、以下、実施の形態１を中心に説明を行う。

【００４２】まず、このシステムのオペレータ又は個人

証の持ち主が、必要な個人情報を、入力手段３２を用いてシステムへ入力する（ステップ１）。次に、ステップ２にて、デジタルカメラ３３により、持ち主を撮影し認証画像を取得する。

【００４３】ステップ３では、制御手段３４が、通信手段４０を用いて、通信網４１を経由し、サーバ４２へ接続する。

【００４４】次に、ステップ４にて、制御手段３４は、通信手段４０を経由し、サーバ４２へ、識別子と、この識別子に対応する透かし情報を生成するように、要求する。

【００４５】これに応じて、サーバ４２側の、識別子生成手段４３は、データベース３をアクセスし、未だ付与されていない新しい識別子を生成し、透かし情報生成手段４４は、この新しい識別子に対応する透かし情報を生成し、これら識別子及び透かし情報が、制御手段３４へ送信される（ステップ５）。

【００４６】制御手段３４は、以上の受信を行うと、透かし情報登録手段３８を用いて、受信した識別子及び透かし情報を、データベース３に登録するように、要求させる（ステップ６）。この要求に応じて、サーバ４２は、これらをデータベース３に記憶させてから、登録済み通知を制御手段３４へ送信する（ステップ７）。

【００４７】制御手段３４は、この通知を受信すると、サーバ４２との接続を解除し（ステップ８）、透かし入り画像作成手段３７へ、受信した透かし情報と、デジタルカメラ３３から得た認証画像とを、渡し、透かし入り画像が作成される（ステップ９）。

【００４８】そして、ステップ１０にて、以上のように作成された、透かし入り画像を書込手段３１へ渡し、書込手段３１は、入出力ポート２４を介し、メモリ２３にこの画像が書き込まれ、必要に応じて、認証画像が、表示部２２に表示できるようになる。これにより、発行処理が完了する。

【００４９】次に、図４を参照しながら、認証処理について説明する。いま、発行済みの個人証１０が読出手段３０にセットされたものとする。まず、読出手段３０は、個人証１０から識別子１１（ここでは「１２３」）を読み出す（ステップ２０）。なお、識別子などの入力は、入力手段３２から行うようにしてもよい。

【００５０】次に、ステップ２１にて、読出手段３０は、入出力ポート１４からメモリ１３に記憶されており、電子透かし情報が埋め込まれているはずの、認証画像を読み出す。

【００５１】次に、ステップ２２にて、制御手段３４は、取得した認証画像を、透かし情報抽出手段３５へ渡し、認証画像から透かし情報の抽出を行わせる。この抽出自体が失敗したときには（ステップ２３）、制御手段３４は、この個人証１０は、不正であると判定し（ステップ２４）、処理を終了する。

【００５２】一方、透かし情報の抽出に成功したときには、制御手段３４は、通信手段４０を用いて、サーバ４２に接続する（ステップ２５）。

【００５３】そして、制御手段３４は、識別子１１を、透かし情報問合手段３９へ渡し、この識別子１１に対応する、透かし情報の問い合わせを行わせる（ステップ２６）。

【００５４】サーバ４２は、この問い合わせを受信すると、データベース３において、この識別子に対応する透かし情報を検索する。サーバ４２は、もし見つからないなら、見つからない旨、見つかったら、見つかった透かし情報を、制御手段３４へ返す（ステップ２７）。

【００５５】制御手段３４は、サーバ４２から受信すると、接続を解除する（ステップ２８）。そして、制御手段３４は、透かし情報が見つからなかった旨受信したときは（ステップ２９）、この個人証１０は、不正であると判定し（ステップ２４）、処理を終了する。

【００５６】一方、制御手段３４は、透かし情報を受信したときは、透かし情報抽出手段３５が抽出した透かし情報と、このときサーバ４２から受信した透かし情報とを、透かし情報比較手段３６へ渡し、比較を行わせる。透かし情報比較手段３６による比較の結果、不一致となったときは、制御手段３４は、この個人証１０は、不正と判定して（ステップ２４）、処理を終了する。

【００５７】一方、この比較の結果、一致を見たときは、制御手段３４は、この個人証１０は、正当であると判定し（ステップ３１）、処理を終了する。

【００５８】また、正当であると判定できたときは、ステップ３２にて、図３の要部と同様の処理をもう一度行い、この識別子に対応する透かし情報を、更新することが望ましい（ステップ３２）。勿論、この更新は、個人証１０の認証画像に埋め込まれる電子透かしの更新と、データベース３における電子透かしの更新との、両方（なお、これらの電子透かしは一致するようにする）を意味する。このようにすると、認証が成功する都度、電子透かしが更新され、一層、改竄に対して堅牢なシステムとすることができる。

【００５９】

【発明の効果】本発明では、個人証の認証画像に埋め込まれた電子透かしを、認証機器で検証することのみに依存するのではなく、この電子透かしを、個人証や認証機器とは、別のデータベースでも記憶しておき、このデータベースの電子透かしとの突き合わせを併用しているため、認証画像の改竄、その他の不正使用に対して、堅牢なシステムを構築できる。

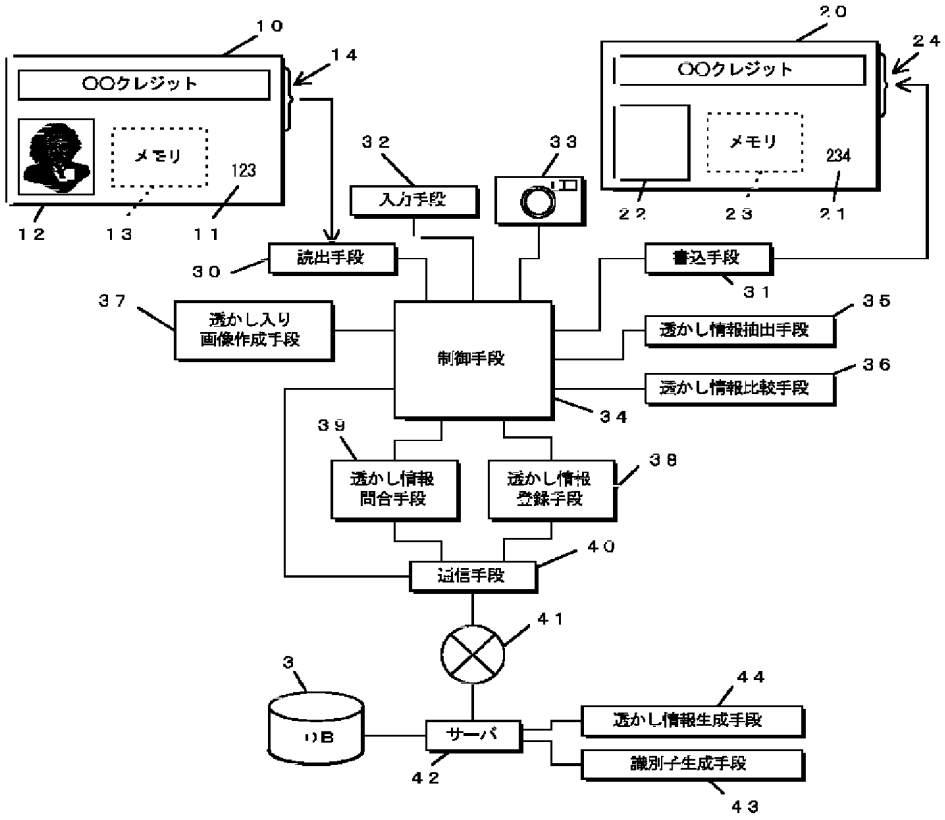
【図面の簡単な説明】

【図１】本発明の実施の形態１におけるシステムのブロック図

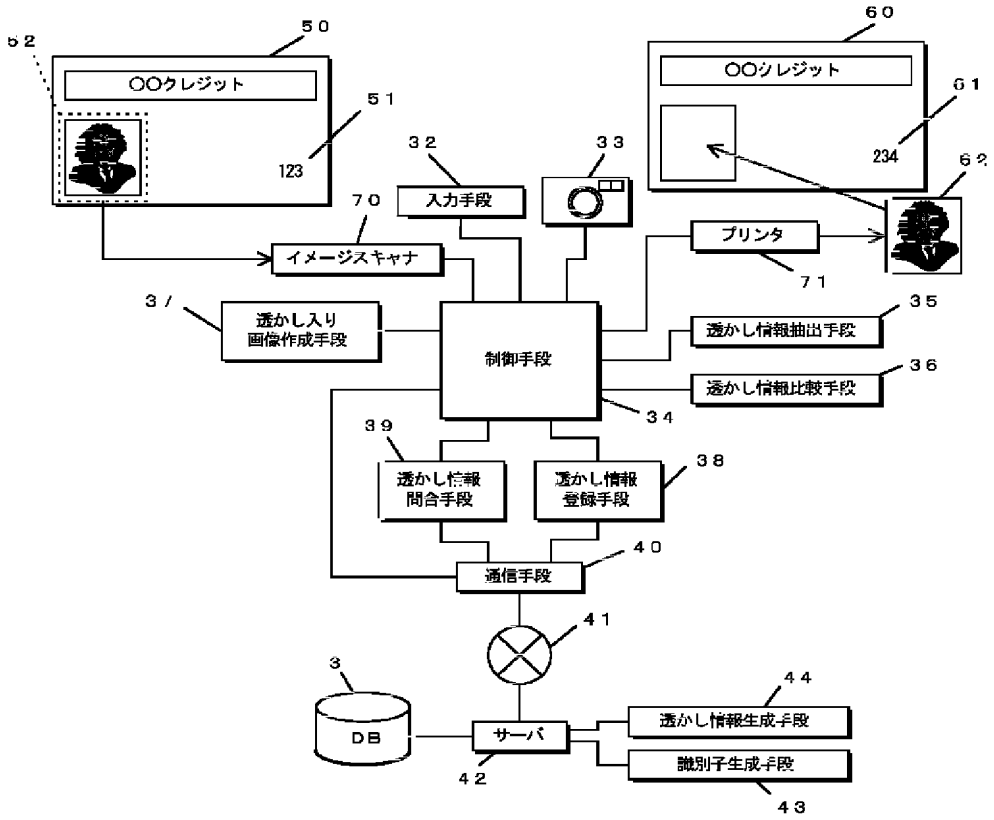
【図２】本発明の実施の形態２におけるシステムのブロック図

【図３】本発明の実施の形態１における発行処理を示すフローチャート
【図４】同認証処理を示すフローチャート
【図５】同個人証、識別子、電子透かし及びデータベースの概略関係図
【符号の説明】
３　データベース
１０、２０　個人証
１１、２１　識別子
１２、２２　表示部
１３、２３　メモリ
３５　透かし情報抽出手段
３６　透かし情報比較手段
３７　透かし入り画像作成手段
３８　透かし情報登録手段
３９　透かし情報問合手段
４２　サーバ
４３　識別子生成手段
４４　透かし情報生成手段

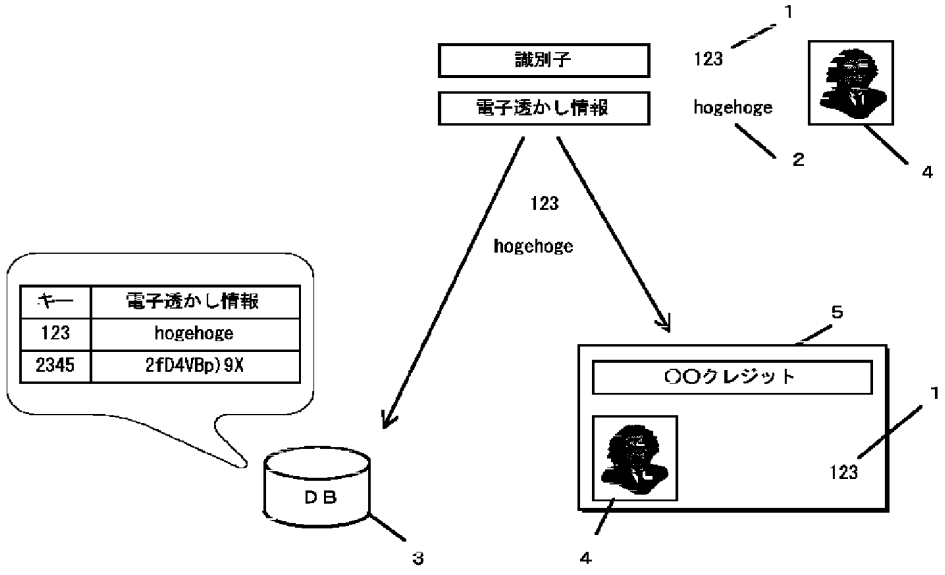
【図１】



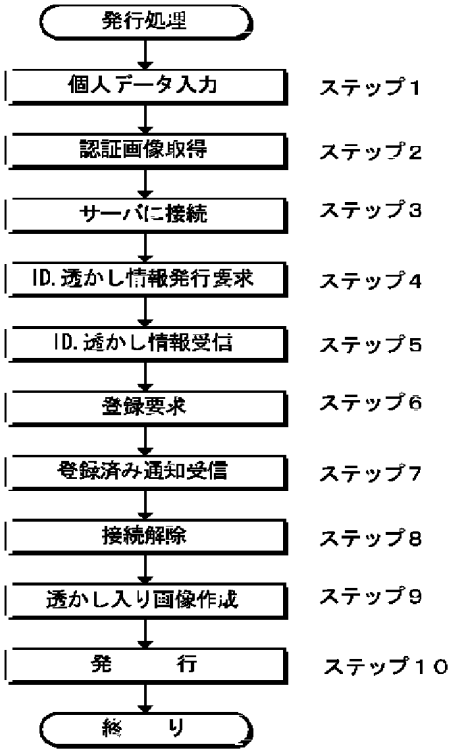
【図２】


５２
５０
○○クレジット
５１
123
３２
入力手段
３３
７０
イメージスキャナ
６０
○○クレジット
６１
234
６２
プリンタ
７１
３７
透かし入り
画像作成手段
制御手段
３５
透かし情報抽出手段
３６
透かし情報比較手段
３４
３９
透かし情報
問合手段
３８
透かし情報
登録手段
４０
通信手段
４１
３
DB
４４
サーバ
透かし情報生成手段
識別子生成手段
４２
４３

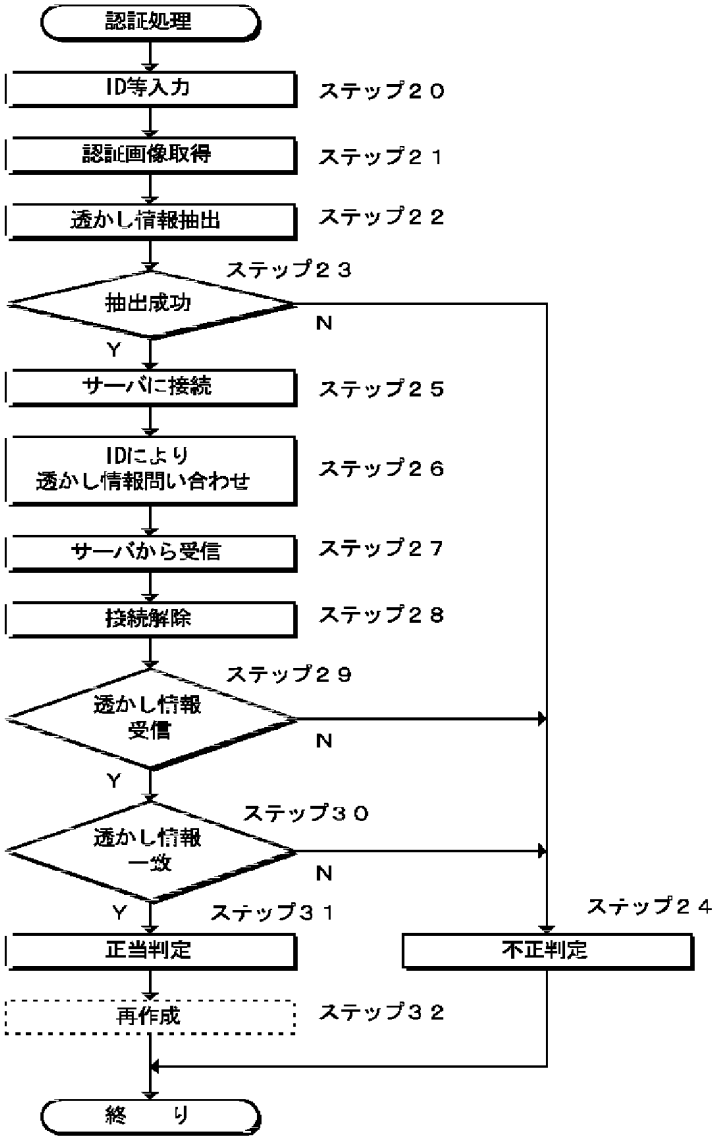
【図５】


識別子
電子透かし情報
1
123
hogehoge
2
4
123
hogehoge
キー
電子透かし情報
123
hogehoge
2345
2fD4VBp)9X
DB
3
5
○○クレジット
1
123
4

【図３】



【図４】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	（参考）
		Ｈ０４Ｌ　9/00	６７３Ｃ

(72)発明者　津森　伸一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　桂　卓史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　井上　尚
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B035 AA14 BB02 BB09 BB11 BC01
CA00
5B058 CA01 CA27 CA31 KA02 KA13
KA31 YA20
5C076 AA02 AA14 BA03 BA04
5J104 AA07 AA14 KA01 NA05 NA34
NA35 NA38 NA41